UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

M.R., individually and on behalf of all others similarly situated, Plaintiffs, v. THOMPSON COBURN, LLP, Defendant.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff M.R. ("Plaintiff M.R.") individually and on behalf of all others similarly situated brings this Class Action Complaint against Defendant Thompson Coburn, LLP ("Defendant") based on personal knowledge the investigation of counsel, and alleges as follows:

NATURE OF THE ACTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms caused to Plaintiff and over 305,000 similarly situated persons[1] (collectively, the "Class" or "Class Members" or "Breach Victims") in a massive and preventable data breach of Defendant's inadequately protected computer network.

2. On May 29, 2024, Defendant first became aware of suspicious activity within its network. Following an investigation, Defendant determined that between May 28 and

[1] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

May 29, 2024, hackers infiltrated and accessed their inadequately protected computer systems.

3. On November 6, 2024, Defendant belatedly reported the hacking incident, which was subsequently posted to the U.S. Department of Health and Human Services' HIPAA Breach Reporting Tool website.[2] The hackers intentionally targeted Defendant to unlawfully access the highly sensitive, confidential, and personal health information of over 305,000 individuals. Defendant has stated that the hacking incident ("Data Breach") affected an undisclosed number of patients of Presbyterian Healthcare Services ("PHS"), a healthcare client of Defendant in New Mexico. However, it remains unclear whether other clients of Defendant were impacted, or if all 305,088 Breach Victims were patients of PHS.

4. Plaintiff's and Class Member's sensitive and private personal information—entrusted to Defendant, its officials, and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach. The personally identifiable information ("PII") and personal health information ("PHI") (collectively "Private Information") compromised in the Data Breach includes names, social security numbers, dates of birth, medical record number, patient account number, prescription and treatment information, clinical information, medical provider information, and health insurance information.

5. Despite identifying the Data Breach as early as May 29, 2024, Defendant did not report the breach until November 6, 2024, approximately five months after the Data

[2] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Breach occurred and the sensitive Private Information of those individuals affected had been exposed.

6. In short, as a result of Defendant's failure to safeguard the Breach Victims' Private Information, hackers gained access to sensitive data that could enable them to carry out various forms of identity theft, jeopardizing the financial and personal lives of hundreds of thousands of individuals.

7. Defendant is a national law firm headquartered in St. Louis, Missouri, with additional offices in major cities like Chicago, Dallas, Los Angeles, New York City, and Washington, D.C. Defendant offers a long list of legal services, including data breach litigation in an array of industries. Defendant employs over 375 attorneys and achieved a record revenue of $245 million in 2022.[3]

8. Defendant's conduct—failing to implement adequate and reasonable measures to protect their computer systems, failing to promptly detect and report the Data Breach, and failing to provide timely and appropriate notice of the Breach—left the victims vulnerable to identity theft. Moreover, by not detecting the breach in a timely manner or alerting the victims, Defendant failed to provide critical warnings that would have allowed individuals to monitor their financial accounts and credit reports, leaving them exposed to the unauthorized use of their sensitive information.

[3] *See* https://www.thompsoncoburn.com/docs/default-source/news-documents/AmLaw_TCRevenueGrowth.pdf.

9. Defendant knew or should have known—given its experience in data breach litigation— that each Breach Victim deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Private Information misuse.

10. Moreover, Defendant knew or should have known that its client, PHS, had experienced at least four data breaches in the past five years, and as a result should have taken proactive measures to prevent cybercriminals from accessing PII from PHS.

11. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a diminution in value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendant, out-of-pocket expenses and the value of their time reasonably incurred to remedy and mitigate the effects of the Data Breach.

12. Armed with the Private Information accessed in the Data Breach, cybercriminals now have the means to commit a wide range of crimes, leaving Plaintiff and the Class exposed to ongoing and imminent risk of various forms of identity theft. This threat will persist for the foreseeable future, as they will be forced to remain extra vigilant—constantly monitoring their financial accounts and personal data—due to Defendant's failures, in an attempt to prevent further victimization for the rest of their lives.

13. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed and/or removed from Defendant's network during the Data Breach.

14. Accordingly, Plaintiff brings this class action lawsuit on behalf of themself and a class of individuals, all of whom are Class Members whose private information was

accessed and/or stolen by cybercriminals due to Defendant's negligent and reckless failure to implement reasonable and up-to-date cybersecurity measures to protect their sensitive data.

PARTIES

15. Plaintiff M.R. is, and at all times relevant hereto has been, a resident of Albuquerque, New Mexico. Plaintiff was a patient of PHS located in Albuquerque, New Mexico, at all times relevant to the Data Breach. Plaintiff learned of the Data Breach through a letter from Defendant.

16. Defendant Thompson Coburn, LLP, is a Missouri limited liability partnership with its headquarters in St. Louis, Missouri. Defendant is a law firm which serves a wide range of industries, offering legal services to clients in over 30 different practice areas. These practice areas include, but are not limited to: Cybersecurity, Privacy and Data Governance, Electrical & Computer Systems, Corporate Governance & Compliance, Consumer Products Litigation, and Blockchain Technology & Digital Currency. Defendant employs over 370 full-time attorneys across its various offices.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

JURISDICTION AND VENUE

18. Plaintiff incorporates by reference all allegations of the preceding paragraphs as fully set forth herein.

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1132(d). The amount in controversy exceeds $5 million, exclusive of interests and costs, there are more than 100 members in the proposed class, and there is minimal diversity because at least one plaintiff and one defendant are citizens of different states.

20. This Court has personal jurisdiction over Defendant because it is headquartered in Missouri, its principal place of business is in Missouri, and it regularly conducts business in Missouri.

21. Venue as to Defendant is proper in this judicial district under 28 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

A. The Data Breach and Defendant's Failure to Timely Disclose the Same

22. Beginning on or around May 28, 2024, through May 29, 2024, unauthorized third-party hackers accessed Defendant's computer system and acquired Plaintiff's and Class Members' Private Information.

23. On May 29, 2024, Defendant became aware of the Data Breach and commenced an investigation. Following its investigation, it was determined that 305,088 individuals were victims of the Data Breach. The investigation further revealed that the information accessed and taken by hackers included information from at least one client, PHS.

24. On November 6, 2024, Defendant issued a notice (the "Notice of Breach" or "Notice") to inform Breach Victims of the Data Breach. The Notice further specified that the compromised files contained protected health and personal information related to certain patients of PHS including names, Social Security numbers, dates of birth, medical record numbers, patient account numbers, prescription and treatment information, clinical details, medical provider information, and health insurance data.[4]

25. Despite detecting the breach in May and knowing that Plaintiff and Class Members were at risk, Defendant took no action to warn the Breach Victims until approximately five months later. During this delay, cybercriminals were able to monitor and exploit their unsuspecting victims, leaving them exposed to fraud and further harm—risks they may have been able to mitigate had Defendant disclosed the data breach in a timely manner.

26. Defendant's Notice was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized third-parties accessed its computer server, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach was as system-wide breach, whether servers storing information were accessed, and how many clients were affected by the Data Breach.

27. Despite the seriousness of the Data Breach, Defendant has taken minimal steps to protect the Breach Victims. While Defendant is offering free access to credit

[4] *See* https://tcnotification.com/.

monitoring and identity theft protection services, the duration of this offer remains unspecified.

28. Defendant failed to properly safeguard Plaintiff and Class Members' personal information, allowing cybercriminals to access this trove of data months before Defendant alerted the Breach Victims to be vigilant.

29. Defendant had obligations created by reasonable industry standards, common law, and its representations to Class Members, to keep Private Information confidential and to protect the information from unauthorized access.

30. Plaintiff and Class Members provided their Personal Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. The Data Breach was clearly foreseeable to Defendant. Defendant's client PHS is a target for cybercriminals who recognize that as healthcare providers, they collect, maintain, and even create Private Information, including protected health information. It is well known that cyber-attacks against healthcare providers such as PHS are targeted and frequent. Such data breaches against healthcare providers have become widespread. In fact, its client PHS has now suffered at least four breaches within the last five years.

32. Moreover, Defendant's client files, which contain sensitive information from individuals and companies across a wide range of industries, would be a prime target for cybercriminals due to the wealth and diversity of the data they contain. These files likely include highly valuable personal, financial, and proprietary information—such as Social

Security numbers, medical records, financial statements, trade secrets, and business strategies—making them a goldmine for identity theft, fraud, and corporate espionage. Cybercriminals seek access to this type of information to exploit vulnerabilities for financial gain, sell it on the dark web, or use it for malicious purposes, such as blackmail or identity theft. The broad scope of industries served by Defendant means that the stolen data could have significant repercussions, impacting not just individual clients but entire businesses, further heightening the appeal of these files to cybercriminals looking for high-value, high-impact targets.

33. Law firms are increasingly vulnerable to data breaches and cyber-attacks due to a range of cybersecurity challenges. One of the most critical weaknesses is their reliance on outdated systems and software. Many firms continue to use legacy technologies that are no longer supported by vendors, exposing them to known security vulnerabilities that cybercriminals can easily exploit. In fact, a study by the American Bar Association revealed that 42% of law firms with 100 or more employees still use outdated software, significantly increasing their risk of a breach.[5] In addition to this, a mere 29% of firms have undergone comprehensive security assessments by third-parties, and only 42% have active incident response plans in place.[6] Further, in 2023, 29% of law firms reported experiencing a "security breach."

B. Plaintiff's Experience Following the Data Breach

[5] *See* https://processbolt.com/insights/blog/why-law-firm-data-breaches-are-skyrocketing-in-2024/.

[6] *See* https://processbolt.com/insights/blog/why-law-firm-data-breaches-are-skyrocketing-in-2024/.

34. Plaintiff entrusted their Private Information to Defendant or one of Defendant's clients, who in turn entrusted the information to Defendant.

35. Plaintiff received a letter from Defendant, dated November 6, 2024, informing them that their name, medical record number, patient account number, prescription/treatment information, clinical information, and medical provider information had been disclosed to an unknown actor as a result of the Data Breach.

36. Plaintiff has spent significant time responding to the dangers from the Data Breach, such as reviewing financial accounts and credit reports with valuable time that could have been spent otherwise.

37. Because the Data Breach was an intentional attack by cybercriminals seeking valuable information that they could exploit, Plaintiff remains at critical risk of severe identity theft and exploitation.

38. Plaintiff is very careful about not sharing their sensitive Private Information. They have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

39. Plaintiff takes great care to store any document containing their personal information in secure locations or to properly dispose of such documents. They also exercise caution by selecting unique usernames and strong passwords for their online accounts to protect their privacy and security.

40. Plaintiff has suffered imminent and ongoing harm due to the significantly heightened risk of fraud, identity theft, and misuse resulting from the unauthorized

exposure of their personal information—particularly their Social Security number—to third parties, including potentially criminal actors.

41. Plaintiff has a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

C. Defendant Had An Obligation to Protect Personal Information Under Federal and State Law and the Applicable Standard of Care

42. Defendant collects, maintains, and stores the Private Information of Plaintiff and the Class in the usual course of business. Defendant frequently engages in data breach litigation. In doing so, Defendant collects the Private Information of its clients and the plaintiffs and class members of other suits.

43. In collecting, maintaining, and storing such Private Information, Defendant promises to keep such information confidential and protect it from third parties.

44. Under the Federal Trade Commission Act ("FTCA," 15 U.S.C. § 45), Defendant was prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has determined that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal information constitutes an "unfair practice" in violation of the Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

45. Defendant is also required by various state laws and regulations to protect Plaintiff's and Class Members' Private Information.

46. In addition to its obligations under federal and state laws, Defendant had a duty to the Breach Victims whose Private Information was entrusted to its care. This duty required Defendant to exercise reasonable care in acquiring, retaining, securing, safeguarding, deleting, and protecting that information from compromise, loss, theft, unauthorized access, or misuse. Defendant owed Plaintiff and the Class Members an obligation to provide reasonable security measures, in line with industry standards and regulatory requirements, ensuring that its computer systems, networks, and personnel responsible for them adequately protected the personal information of Plaintiff and the Class Members from unauthorized exposure.

47. Defendant owed a duty to Plaintiff and the Class Members, whose personal information was entrusted to its care, to design, maintain, and regularly test its computer and email systems to ensure that the Private Information in its possession was adequately secured and protected from unauthorized access or compromise.

48. Defendant owed a duty to Plaintiff and the Class Members, whose Private Information was entrusted to its care, to establish and enforce reasonable data security practices and procedures to protect that information. This duty included properly training its employees and others with access to personal information within its computer systems on how to securely handle and protect such data.

49. Defendant owed a duty to Plaintiff and the Class Members, whose personal information was entrusted to its care, to implement processes capable of detecting a breach in its data security systems in a timely manner.

50. Defendant owed a duty to Plaintiff and the Class Members, whose personal information was entrusted to its care, to disclose if its computer systems and data security practices were inadequate to protect individuals' personal information from theft. Such an inadequacy would constitute a material fact in the decision to entrust personal information to Defendant.

51. Defendant owed a duty to Plaintiff and the Class Members, whose personal information was entrusted to its care, to promptly and accurately disclose any data breaches that occurred.

52. Defendant owed a duty of care to Plaintiff and the Class Members, as they were foreseeable and likely victims of any deficiencies in the Defendant's data security practices.

D. Defendant Was on Notice of Cyber Attack Threats and the Inadequacy of Its Data Security

53. In the years leading up to the Data Breach, Defendant knew or should have known that its computer systems were targets for cybersecurity attacks, as warnings and guidance on the risks were widely available and easily accessible online.

54. In fact, Defendant itself has published warnings and guidance on the risks of data breaches on its own website, underscoring its awareness of these threats.[7] A blog post from September 2016, titled "Don't Doubt the Data Breach: Massive Yahoo Hack Reminds

[7] *See* https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes?tag=data-breach.

Us It's Not If, But When,"[8] serves as a stark reminder of the growing cybersecurity risks. The article specifically emphasizes the critical need for companies to "preemptively create and test their breach-response program," illustrating Defendant's own understanding of the heightened risk of data breaches long before it fell victim to one itself. This makes Defendant's failure to act on its own advice all the more glaring.

55. Moreover, Defendant's security declaration appears to have unwittingly predicted the very incident that transpired here. Specifically, the statement provides:

56. No security system is impenetrable; and, because the internet is an open global communications vehicle, we cannot and do not guarantee that information, during transmission through the internet or while stored on our systems or otherwise, will be absolutely safe from intrusion by others, such as hackers.[9] In addition to Defendant's clear awareness of cyber-attack threats, government agencies such as the Federal Bureau of Investigation ("FBI") regularly issue warnings and publish resources aimed at addressing the escalating risk of these attacks. For instance, the FBI's *Ransomware Prevention and Response for CISOs* manual highlights the alarming rise in ransomware incidents, stating that "Ransomware is the fastest-growing malware threat, targeting users of all types…[o]n average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016."[10]

---

[8] *See* https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2016-09-22/don-t-doubt-the-data-breach-massive-yahoo-hack-reminds-us-it-s-not-if-but-when.

[9] *See* https://www.thompsoncoburn.com/firm/privacy#:~:text=We%20may%20collect%20personal%20information,%2C%20fax%20number%2C%20and%20preferences.

[10] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

57. In October 2019, the FBI published an online article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" which warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[11]

58. In September 2020, the United States Cybersecurity and Infrastructure Security Agency ("CISA") released a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[12]

59. Given the increasing and evolving nature of cyber threats, CISA published and updated versions of its 'Ransomware Guide" guide in both May and September of 2023. These revisions include, but are not limited to, enhanced guidance on hardening Server Message Blocks (SMB), new recommendations for securing web browsers, and additional information about the growing threat of cybercriminals impersonating employees to gain unauthorized access.[13]

60. In January 2023, the Identity Theft Resource Center ("ITRC"), a nationally recognized nonprofit organization established to support victims of identity crime, released

[11] https://www.ic3.gov/PSA/2019/psa191002.
[12] https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.
[13] *See* https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf.

its Annual Data Breach Report. According to ITRC's report, there were 3,205 reported "data compromises" in 2023, marking a 78% increase compared to 2022.[14]

61. In December 2023, the American Bar Association reported that the percentage of law firms that had experienced a security breach had risen to 29%, reflecting a 2% increase from the previous year. The article, among other things, specifically states that "[c]ybersecurity should be top-of-mind for every attorney" and that "[c]ybersecurity awareness training for employees should be performed once a year at a minimum considering threats, vulnerabilities, and attack methods."[15] In New York City, where Defendant has an office, the New York State Bar Association requires attorneys to complete one continuing legal education ("CLE") credit in cybersecurity, privacy, and data protection.[16]

62. This readily accessible information confirms that, prior to the data breach, Defendant knew or should have known that: (i) cybercriminals were actively targeting companies like Defendant and its clients, (ii) these attackers were increasingly aggressive in pursuing organizations holding large amounts of sensitive data, (iii) cybercriminals were

[14] https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/#:~:text=According%20to%20the%202023%20Annual,100%20percent%20to%2054%20percent.
https://www.americanbar.org/groups/law_practice/resources/tech-report/2023/2023-cybersecurity-techreport/.

[15] https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2024/ensuring-security-protecting-your-law-firm-and-client-data/.

[16] New York CLE Requirements, New York State Bar Association, https://nysba.org/new-york-cle-requirements/?srsltid=AfmBOopU9dQtZwp4sCwOVP6HLUnqckxds5_7O5c5wxUkajB249ILqiAg (last visited Nov. 11, 2024).

leaking corporate information on dark web platforms, and (iv) their tactics included threatening to publicly release stolen data.

E. Defendant Could Have and Should Have Prevented this Data Breach

63. For legal professionals, it's no longer acceptable to wait for a problem to arise before addressing it. As the FBI emphasizes, "proactive prevention is the best defense."[17] This approach involves staying ahead of emerging threats and ensuring that employees are regularly trained to recognize and respond to potential risks.

64. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by the FBI:

- **Implement an awareness and training program:** Educate employees and individuals about the threat of ransomware and how it is delivered, as end users are often the primary targets.
- **Enable strong spam filters:** Prevent phishing emails from reaching end users by using technologies like Sender Policy Framework ("SPF"), Domain Message Authentication Reporting and Conformance ("DMARC"), and DomainKeys Identified Mail (DKIM) to block email spoofing.
- **Scan all incoming and outgoing emails:** Detect threats by scanning emails and filtering executable files to prevent them from reaching end users.
- **Configure firewalls:** Block access to known malicious IP addresses to prevent unauthorized access.
- **Patch operating systems, software, and firmware:** Regularly update and patch devices, potentially using a centralized patch management system for greater efficiency.
- **Set anti-virus and anti-malware programs for regular scans:** Ensure these programs run automatic scans to detect and remove potential threats.

[17] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- **Manage privileged accounts based on the principle of least privilege:** Limit administrative access to users only when absolutely necessary, and ensure those with admin privileges use them only when required. Implement an awareness and training program.

- **Configure access controls:** Implement least privilege principles for file, directory, and network share permissions. Users should only have access to what they need—if a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- **Disable macro scripts in office files transmitted via email:** Prevent the execution of potentially harmful macros by disabling them in office files sent via email. Consider using Office Viewer software instead of full office suite applications to open email attachments.

- **Implement Software Restriction Policies (SRP):** Use SRPs or similar controls to prevent programs from executing from common ransomware locations, such as temporary folders associated with web browsers or compression programs, including the AppData/LocalAppData folder.

- **Disable Remote Desktop Protocol (RDP):** If RDP is not in use, consider disabling it to reduce potential attack vectors.

- **Use application whitelisting:** Allow only programs that are explicitly permitted by security policy to execute, blocking any unauthorized or potentially malicious software.

- **Execute operating system environments or specific programs in a virtualized environment:** Run sensitive systems or programs in isolated virtual environments to reduce risk.

- **Categorize data based on organizational value:** Implement physical and logical separation of networks and data for different organizational units to protect critical information and ensure appropriate access control.

65. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by the Joint

Ransomware Task Force's ("JRTF") #StopRansomware Guide, although this list does not encompass the full range of recommended actions:

- **Conduct regular vulnerability scanning to identify and address** vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

- **Regularly patch and update software and operating systems to the latest available versions.** Prioritize timely patching of internet-facing servers-that operate software for processing internet data such as web browsers, browser plugins, and document readers-especially for known exploited vulnerabilities….

- **Limit the use of RDP and other remote desktop services.** If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client.

- **Ensure all on-premises, cloud services, mobile, and personal devices are properly configured, and security features are enabled**. For example, disable ports and protocols that are not being used for business purposes.[18]

66. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by the FTC in its latest update to *Protecting Personal Information: A Guide for Business*:

- Know what personal information you have in your files and on your computers

- Keep only what you need for your business

- Protect the information that you keep

[18] *See* #StopRansomware Guide, https://www.cisa.gov/resources-tools/resources/stopransomware-guide.

- Properly dispose of information you no longer need
- Create a plan to respond to security incidents.[19]

67. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by Microsoft's 2023 Digital Defense Report:

- **Enable multifactor authentication (MFA)**. This protects against compromised user passwords and helps to provide extra resilience for identifies.
- **Apply Zero Trust principles.** This includes ensuring users and devices are in a good state before allowing access to resources, allowing only the privilege that is needed for access to a resource and no more, assuming system defenses have been breached and systems may be compromised.
- **Use extended detection and response (XDR) and antimalware**. Implement software to detect and automatically block attacks and provide insights into the security operations software.
- **Keep up to date**. Unpatched out-of-date systems are a key reason many organizations fall victim to cyber-attacks.
- **Protect data**. Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.[20]

68. Given that Plaintiff and Class Members provided Private Information to Defendant or one of Defendant's clients, which entrusted the information to Defendant,

[19] *See* Protecting Personal Information: A Guide for Business, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[20] *See* Microsoft Digital Defense Report 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

Defendant should have and could have taken the above measures to ensure that the Private Information was safe from unauthorized actors.

F. Defendant Failed to Comply with FTC Guidelines

69. Defendant was also prohibited by the FTCA (15 U.S.C. § 45), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has determined that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal information constitutes an "unfair practice" in violation of the Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236.

70. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

71. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

72. The FTC recommends that companies retain information only for as long as necessary to authorize a transaction, limit access to sensitive data, enforce the use of strong, complex passwords on networks, adopt industry-recognized security practices,

continuously monitor for suspicious activity on the network, and verify that third-party service providers have implemented appropriate security measures.

73. The FTC has taken enforcement actions against businesses for failing to adequately protect consumer data, treating the failure to implement reasonable and appropriate safeguards against unauthorized access to sensitive consumer information as an unfair practice prohibited by Section 5 of the FTCA (15 U.S.C. § 45). The resulting orders from these actions provide further clarity on the specific measures businesses must adopt to fulfill their data security obligations.

74. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

G. Plaintiffs and Class Members Suffered Damages

75. The ramifications of Defendant's failure to keep the Private Information of Plaintiff and Class Members secure are long-lasting and severe. In 2023 alone, American adults lost $43 billion to identity theft.[21] Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

76. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing,

[21] https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html#:~:text=American%20adults%20lost%20a%20total,new%20report%20cosponsored%20by%20AARP.

safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized third parties.

77. Defendant further owed and breached its duty to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own systems.

78. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse of Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff and Class Member are now at a heightened risk of identity theft and fraud.

79. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their name and credit score. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of the negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

80. Additional risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

81. The Private Information of individuals is of high value to criminals. According to research by numerous sources, an individual's Private Information can be

worth over $1,000 on the dark web, with details like online banking logins selling for around $100, full credit card details ranging from $10-$100, and a complete set of documents for identity theft costing close to $1,000.[22]

82. The information compromised in the Data Breach is far more valuable than typical data, such as credit card information, because victims can quickly mitigate damage by canceling or closing accounts. In contrast, the compromised data—such as medical record numbers, patient account details, prescription information, clinical data, and health insurance records—holds significant value for criminals due to its potential use in identity theft, medical fraud, and extortion.

83. Moreover, the process of replacing a Social Security number is both time consuming and difficult. According to the Social Security Administration, if your Social Security number is lost or stolen but there's no evidence of misuse, you cannot obtain a new number.[23] This leaves victims in a precarious situation, essentially forced to wait for fraud to occur before they can take action to mitigate the damage. This delay in being able to change a compromised Social Security number puts victims at continued risk for identity theft, financial fraud, and other forms of exploitation, making it much harder to protect themselves in the aftermath of a data breach.

84. As a result of the Data Breach, Plaintiff's and Class Members' Private Information has diminished in value.

[22] https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.
[23] https://www.ssa.gov/pubs/EN-05-10064.pdf.

85. The Private Information belonging to Plaintiff and Class Members is sensitive, personal in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standard.

86. The Data Breach was a direct and proximate result of Defendant's failure to: (i) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices and common law; (ii) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (iii) protect against reasonably foreseeable threats to the security or integrity of such information.

87. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement proper data security measures, despite its obligation to protect Plaintiff's and Class Members' Private Information.

88. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

89. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and

family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

90. Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Defendant's Breach Notice indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

91. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at an increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as

Defendant fails to undertake appropriate measures to protect the Private Information in their possession; and

e. Anxiety and distress resulting from fear of misuse of their Private Information.

92. In addition to a remedy for economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ALLEGATIONS

93. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

94. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a) and 23(b)(3), Plaintiff asserts all claims on behalf of a Class defined as follows:

> All persons whose Private Information was compromised by the Data Breach discovered on or about May 29, 2024, including all who were sent a notice of the Data Breach.

95. Members of the Class are sometimes, where appropriate, referred to herein collectively as "Class Members" or the "Classes."

96. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

97. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

98. **Numerosity**: The proposed Class is so numerous that joinder of all members is impracticable. Defendant reported to the United States Department of Health and Human Services HIPAA Breach Reporting Tool website that approximately 305,088 individuals were affected by the Data Breach.[24]

99. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the class include:

a. Whether Defendant failed to adequately safeguard Plaintiff's and the Classes' Private Information

b. Whether Defendant failed to protect Plaintiff's and the Class' Private Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and the Class' Private Information violated the FTCA, state laws, and/or Defendant's other duties;

d. Whether Defendant violated the data security statutes and data breach notification statutes applicable to Plaintiff and the Class;

[24] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

e. Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach expeditiously and without unreasonable delay after the Data Breach was discovered;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Breach Victims' Private Information properly as promised;

g. Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class' Private Information;

h. Whether Defendant entered into implied contracts with Plaintiff and the members of the Class that included contract terms requiring Defendant to protect the confidentiality of Personal Information and have reasonable security measures;

i. Whether Defendant violated the consumer protection statutes, data breach notification statutes, and state privacy statues applicable to Plaintiff and the Class;

j. Whether Defendant failed to notify Plaintiff and Breach Victims about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

k. Whether Defendant's conduct described herein constitutes a breach of their implied contracts with Plaintiff and the Class;

l. Whether Plaintiff and members of the Class are entitled to damages as a result of Defendant's wrongful conduct;

m. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n. What injunctive relief is appropriate to redress the imminent and current ongoing harm faced by members of the Class.

100. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

101. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and [his/her] counsel are committed to prosecuting this action vigorously on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of other members of the Class.

102. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class.

103. **Policies Generally Applicable to the Class**: This case is appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Plaintiff and the proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members

of the Class and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant' practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiffs' challenge to those practices hinges on Defendant' conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

104. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant' conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT ONE
Negligence
(On Behalf of Plaintiff and the Class)

105. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

106. Defendant solicited, gathered, and stored the Private Information of Plaintiff and the Class.

107. Defendant knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiff and the Class and the importance of adequate security.

108. Defendant was well aware of the fact that hackers routinely attempt to access Private Information without authorization. Defendant also knew about numerous, well-publicized data breaches wherein hackers stole the Private Information from companies who held or stored such information.

109. Defendant owed duties of care to Plaintiff and the Class whose Private Information was entrusted to it. Defendant's duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;

b. To protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly train its employees to avoid phishing emails;

d. To use adequate email security systems, including DMARC enforcement and SPF enforcement, to protect against phishing emails;

e. To adequately and properly train its employees regarding how to properly and securely transmit and store Private Information;

f. To train its employees not to store Private Information in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

110. Because Defendant knew that a security incident, breach or intrusion upon its systems would potentially damage thousands of its current and/or former clients and employees, including Plaintiff and Class Members, it had a duty to adequately protect their Private Information.

111. Defendant owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

112. Defendant knew, or should have known, that its security practices and computer systems did not adequately safeguard the Private Information of Plaintiff and the Class

113. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard the Private Information of Plaintiff and the Class.

114. Defendant breached its duty of care by failing to provide prompt notice of the Data Breach to persons whose Private Information was compromised.

115. Defendant acted with reckless disregard for the security of the Private Information of Plaintiff and the Class because Defendant knew or should have known that their computer systems and data security practices were not adequate to safeguard the Private Information that it collected and stored, which hackers were attempting to access.

116. Defendant acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the Data Breach so that they could take measures to protect themselves from damage caused by the fraudulent use of Private Information compromised in the Data Breach.

117. Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class' willingness to entrust Defendant with their personal information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the Private Information therein and to implement security practices to protect the Private Information that it collected and stored from attack.

118. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to:

a. Secure its employees' email accounts;

b. Secure access to its servers;

c. Comply with current industry standard security practices;

d. Encrypt Private Information during transit and while stored on Defendant's systems;

e. Properly and adequately train their employees on proper data security practices;

f. Implement adequate system and event monitoring;

g. Implement the systems, policies, and procedures necessary to prevent hackers from accessing and utilizing Private Information transmitted and/or stored by Defendant;

h. Undertake periodic audits of record-keeping processes to evaluate the safeguarding of Private Information;

i. Develop a written records retention policy that identifies what information must be kept and for how long;

j. Destroy all discarded employee information, including information on prospective employees, temporary workers, subcontractors, and former employees;

k. Secure Private Information and limit access to it to those with a legitimate business need;

l. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used to manage e-mail, internet use, and so forth;

m. Avoid using Social Security numbers as a form of identification; and

n. Have a plan ready and be in a position to act quickly should a theft or data breach occur.

119. Defendant also had independent duties under federal and state law requiring them to reasonably safeguard Plaintiff's and the Class' Private Information and promptly notify them about the Data Breach.

120. Defendant breached the duties they owed to Plaintiff and Class members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect the Private Information of Plaintiff and the Class both before and after learning of the Data Breach;

c. By failing to comply with minimum industry data security standards before, during, and after the period of the Data Breach; and

d. By failing to timely and accurately disclose that the Private Information of Plaintiff and the Class had been improperly acquired or accessed in the Data Breach.

121. But for Defendant's wrongful and negligent breach of the duties it owed Plaintiff and the Class Members, their Private Information either would not have been compromised or they would have been able to prevent some or all of their damages.

122. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of further harm.

123. The injury and harm that Plaintiff and Class members suffered (as alleged above) was reasonably foreseeable.

124. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

125. Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT TWO
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

126. Plaintiff incorporates by reference all allegations from the preceding paragraphs as if fully set forth herein.

127. Under the FTCA, 15 U.S.C. § 45, Defendant had a duty to maintain fair and adequate computer systems and data security to protect the Private Information of Plaintiff and the Class.

128. The FTCA prohibits "unfair... practices in or affecting commerce," which includes, as interpreted and enforced by the FTC, the unfair practice of failing to implement reasonable measures to protect Private Information. The FTC publications and orders mentioned above also contributed to the basis of Defendant's duty in this regard.

129. Defendant solicited, collected, and stored the Private Information of Plaintiff and the Class as part of its business activities involving the manufacturing, selling, and installation of gutter protection systems, which affects commerce.

130. Defendant violated the FTCA by failing to implement reasonable measures to protect the Private Information of Plaintiff and the Class, and by not adhering to applicable industry standards, as described herein.

131. Defendant breached its duties to Plaintiff and the Class under the FTCA and various state data security and privacy statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Breach Victims' Private Information.

132. Defendant's failure to comply with relevant laws and regulations constitutes negligence *per se*.

133. Plaintiff and the Class are within the class of persons the FTCA was intended to protect.

134. The harm caused by the Data Breach is the type of harm that the FTCA and state data breach privacy statutes were designed to prevent.

135. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class' Personal Information.

136. Defendant breached its duties to Plaintiff and the Class by negligently and unreasonably delaying the provision of notice regarding the Data Breach, failing to provide such notice expeditiously or as soon as practicable.

137. Defendant's violation of the FTCA, state data security statutes, and/or state data breach notification statutes constitute negligence *per se*.

138. As direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach by, *inter alia,* having to spend time reviewing their accounts and credit reports for unauthorized activity; spend time and incur costs the place a re-new "freeze" on their credit; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

139. The injury and harm that plaintiff and class members suffered (all alleged above) was the direct and proximate result of Defendant's negligence *per se*.

COUNT THREE
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

140. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

141. By requiring Plaintiff and the Class Members Private Information to engage Defendant's legal services, Defendant entered into an implied contract in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff and Class Members' Private Information. In return, Defendant provided Plaintiff and Class Members with legal services.

142. Based on this implicit understanding, Plaintiff and the Class accepted Defendant's offers and provided Defendant with their Private Information.

143. Plaintiff and Class members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information as promised.

144. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

145. Defendant breached the implied contracts by failing to safeguard Plaintiff and Class Members' Private information.

146. Defendant also breached the implied contracts when it engaged in acts and/omissions that are declared unfair trade practices by the FTC. These acts and omissions included (i) representing, either expressly or impliedly, that it would maintain adequate data privacy and security practices and procedures to safeguard the Private Information from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Private Information; and (iii) failing to disclose to the nursing programs and the Class at the time they provided their Private Information that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

147. The losses and damages Plaintiff and Class members sustained were the direct and proximate result of the Defendant's breach of the implied contract with Plaintiff and Class members.

COUNT FOUR
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged herein.

149. A relationship existed between Plaintiff, Class Members and Defendant in which Plaintiff and the Class entrusted Defendant with their Private Information, relying on Defendant's own privacy statement that it "takes your privacy seriously" to safeguard it. By accepting and retaining this sensitive information, there was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

150. Plaintiff and the Class Members entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and refrain from disclosing their Private Information to unauthorized third-parties.

151. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individuals Private Information involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third-party.

152. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing defendant's security protocols to ensure that Plaintiff's and the Class' Private Information in Defendant's possession was adequately secured and protected.

153. Defendant also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class' Private Information. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Defendant was entrusted with Plaintiff and the Class' Private Information.

154. Defendant breached its fiduciary duty that it owed to Plaintiff and the Class by failing to act in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the Private Information of Plaintiff and the Class Members.

155. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort,

and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

156. Defendant's breach of fiduciary duties was the legal cause of damages to plaintiff and the Class Members.

157. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiff and the Class.

158. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class Members have suffered and will continue to suffer from other forms of injury and/or harm, and other economic and non-economic.

COUNT FIVE
Breach of Confidence
(On Behalf of Plaintiff and the Class)

159. Plaintiffs incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

160. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of the Private Information provided by Plaintiff and the Class Members to Defendant, either directly or through Defendant's clients.

161. As alleged herein and above, Defendant's relationship with Plaintiff and the Class Members was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and

would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

162. Plaintiff and Class Members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

163. Plaintiff and Class Members provided their respective Private Information to Defendant's clients, and by proxy to Defendant, with the explicit and implicit understandings that Defendant would take precautions to protect their Private Information from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

164. Defendant voluntarily received in confidence Plaintiff's and the Class Members' Private Information with the understanding that the information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

165. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, by, *inter alia*, not following the best security practices to secure Plaintiff and Class Members' Private Information, Plaintiff and the Class Members' Private Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated

by, released to, stolen by, used by, and/or viewed by unauthorized third-parties and without their express permission.

166. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class Members have suffered damages as alleged herein.

167. But for Defendant's failure to maintain and protect Plaintiff's and Class Member's Private Information in violation of the Parties' understanding of confidence, their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties. Defendant's Data Breach was the direct and legal cause of the misuse of Plaintiff and Class Members' Private Information, as well as the resulting damages.

168. The injury and harm Plaintiff and the Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class Members' Private Information. Defendant knew or should have known its methods of accepting and storing Plaintiff's and the Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class Members' Private Information.

169. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class Members, Plaintiff and the Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to decide how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk of exposure to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former clients; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

170. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. That the Court certify this action as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff are a proper class and sub-class representatives; and appoint Plaintiff's Counsel as Class Counsel;

b. That the Court grant permanent injunctive relief to prohibit Defendant from engaging in the unlawful acts, omissions, and practices described herein;

c. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as it just and proper in an amount to be determined at trial;

d. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

e. That Plaintiffs be granted the declaratory relief sought herein;

f. That the Court award pre- and post-judgment interest at the maximum legal rate; and

g. That the Court grant all such other relief as it deems just and proper.

Dated: November 15, 2024,

Respectfully submitted,

Maureen M. Brady MO#57800
Lucy McShane MO#57957
MCSHANE & BRADY, LLC
4006 Central Street
Kansas City, MO 64111
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

GEORGE FELDMAN MCDONALD, PLLC
Lori G. Feldman, Esq. (*pro hac vice* forthcoming)
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
lfeldman@4-justice.com
eservice@4-justice.com

Attorneys for Plaintiff and the Putative Class